investigation. Specifically, from my experience investigating public corruption offenses, I know that individuals who participate in offenses such as the Subject Offenses may communicate about known government investigations and tailor their stories to be consistent, and tamper with or hide potential evidence. Accordingly, premature disclosure of the scope of this investigation would undermine efforts to obtain truthful statements from relevant witnesses, and could lead to witness tampering and/or obstruction of justice. In addition, if the subjects of this investigation were alerted to the existence of a criminal investigation, it may prompt them to delete electronic records, including in e-mail accounts or other electronic media not presently known to the government. Accordingly, there is reason to believe that, were the Provider to notify the subscriber or others of the existence of the warrant, the investigation would be seriously jeopardized.

28. Additionally, while the Subject Accounts are registered to an enterprise domain ([redacted]), there is no representative of the enterprise that could be notified without seriously jeopardizing the investigation. Indeed, as described above, the subscribers of the Subject Accounts are the CEO and COO of the enterprise, the enterprise itself appears to be an instrumentality of the fraudulent scheme, and there is no known employee of the enterprise or a legal representative that could be notified without jeopardizing the investigation. Pursuant to 18 U.S.C. § 2705(b), I therefore respectfully request that the Court direct the Provider not to notify any person, including any representative of the enterprise domain fraudguarantee.com, of the existence of the warrant for a period of one year from issuance, subject to extension upon application to the Court, if necessary.

29. For similar reasons, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrant and affidavit as

need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

V. Conclusion

30. Based on the foregoing, I respectfully request that the Court issue the warrant sought herein pursuant to the applicable provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) (for contents) and § 2703(c)(1)(A) (for records and other information), and the relevant provisions of Federal Rule of Criminal Procedure 41.

[redacted]

Sworn to before me this
12th day of December, 2019

HONORABLE J. PAUL OETKEN
United States District Judge
Southern District of New York

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All Content and Other Information Associated with the Email Accounts [redacted] and [redacted] Maintained at Premises Controlled by Google, LLC, USAO Reference No. [redacted]

19 MAG 11651

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: Google, LLC ("Provider")

Federal Bureau of Investigation and United States Attorney's Office for the Southern District of New York

1. Warrant. Upon an affidavit of Special Agent [redacted] of the Federal Bureau of Investigation, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe the email accounts [redacted] and [redacted] maintained at premises controlled by Google, LLC, contain evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 30 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A. The Government is required to serve a copy of this Warrant and Order on the Provider within 14 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence, and/or tamping with potential witnesses, or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that the Provider shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person, including but not limited to a representative of the enterprise domain, for a period of one year from the date of this Order, subject to extension upon application to the Court if necessary, except that Provider may disclose this Warrant and Order to an attorney for Provider for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

Dec. 12, 2019 3:03 PM
Date Issued Time Issued

HONORABLE J. PAUL OETKEN
United States District Judge
Southern District of New York

Email Search Attachment A

I. Subject Accounts and Execution of Warrant

This warrant is directed to Google, LLC (the "Provider"), headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043, and applies to all content and other information within the Provider's possession, custody, or control associated with the email accounts [redacted] and [redacted] (the "Subject Accounts"). The Provider is directed to produce the information described below associated with the Subject Accounts, limited to content created, sent, or received on or after September 1, 2013 through the date of this warrant.

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

II. Information to be Produced by the Provider

To the extent within the Provider's possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Accounts (subject to the time period limitation set forth above):

a. *Email content.* All emails sent to or from, stored in draft form in, or otherwise associated with the Subject Accounts, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email).

b. *Address book information.* All address book, contact list, or similar information associated with the Subject Accounts.

c. *Subscriber and payment information.* All subscriber and payment information regarding the Subject Accounts, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

d. *Transactional records.* All transactional records associated with the Subject Accounts, including any IP logs or other records of session times and durations.

e. *Google Drive Content.* All Google Drive records associated with the Subject Accounts, including all documents and other records stored on the Google Drive accounts.

f. *Google Docs.* All Google Docs records associated with the Subject Accounts, including all documents created or stored in Google Docs.

g. *Google Calendar.* All calendar entries and records associated with the Subject Accounts.

h. *Location History.* All location records associated with the Subject Accounts.

i. *Information Regarding Linked Accounts, Including Accounts Linked by Cookie.* Any information identifying accounts that are associated or connected to the Subject Accounts, including specifically by Cookie, email account, phone number, Google Account ID, Android ID, or other account or device identifier.

j. *Device Information.* Any information identifying the device or devices used to access the Subject Accounts, including a device serial number, a GUID or Global Unique Identifier, a phone number, serial numbers, MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber

Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI"), and any other information regarding the types of devices used to access the Subject Accounts;

k. *Android Services.* All records relating to Android services associated with the Subject Accounts.

l. *Preserved or backup records.* Any preserved or backup copies of any of the foregoing categories of records, whether created in response to a preservation request issued pursuant to 18 U.S.C. § 2703(f) or otherwise.

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1343 (wire fraud) and § 1349 (attempting and/or conspiring to commit wire fraud) (the "Subject Offenses"), including the following:

a. Evidence relating to, including communications with, Rudolph Giuliani, [redacted] and any actual or potential investors, members, or partners of Fraud Guarantee;

b. Evidence relating to Fraud Guarantee's plans, finances, assets, and operations, or lack thereof, including any corporate books and records;

c. Evidence relating to Fraud Guarantee's actual or prospective business relationships, including but not limited to business relationships with any insurance carriers;

d. Evidence relating to false and fraudulent representations made to potential or actual investors, including drafts of any corporate documents and related materials;

e. Evidence relating to Fraud Guarantee's members, officers, directors, investors, partners, employees, agents, consultants, affiliates, subsidiaries, and associates.

f. Evidence relating to the nature and extent of Rudolph Giuliani's and [redacted] work on behalf of Parnas, Correia, and/or Fraud Guarantee, or lack thereof, including any evidence of Giuliani's efforts to assist in the removal of Ambassador [redacted] and whether or not such efforts benefited Fraud Guarantee;

g. Evidence relating to any efforts by Parnas, Correia, their family members, or others associated with Fraud Guarantee in receiving, transferring, withdrawing, or otherwise using any monetary funds or instruments;

h. Evidence relating to the use of monetary funds or instruments paid to Fraud Guarantee, Parnas, or Correia to make political contributions;

i. Evidence of meetings between Parnas, Correia, Giuliani, and any actual or potential investors in Fraud Guarantee, including but not limited to travel records, and location and IP records;

j. Evidence of the existence of email accounts, iCloud accounts, or electronic devices used by Parnas, Correia or others associated with Fraud Guarantee to communicate with actual or potential investors, or co-conspirators;

k. Passwords or other information needed to access user's online accounts.

Exhibit 1

AO 93 (SDNY Rev. 01/17) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

the Contents of Four iCloud Accounts Currently Located on a Hard Drive Containing the Results of A Prior iCloud Search Warrant

Case No. 19 MAG 8632

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Southern District of New York
(identify the person or describe the property to be searched and give its location):

See Attachment A

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

See Attachment A

The search and seizure are related to violation(s) of *(insert statutory citations)*:

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before November 4, 2019
(not to exceed 14 days)

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the Clerk of the Court.

☑ Upon its return, this warrant and inventory should be filed under seal by the Clerk of the Court. JPO
USMJ Initials

☑ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☑ for 30 days *(not to exceed 30)*.

☐ until, the facts justifying, the later specific date of _____.

Date and time issued: Oct. 21, 2019 10:38 a.m.

Judge's signature

City and state: New York, New York

J. Paul Oetken, United States District Judge
Printed name and title

AO 93 (SDNY Rev. 01/17) Search and Seizure Warrant (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the Court.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

Attachment A

I. Device to be Searched

The device to be searched (the "Subject Device") is described as a hard drive containing the contents of the below four iCloud accounts, which were obtained pursuant to a search warrant authorized on or about May 16, 2019, by the Honorable Stewart Aaron, Magistrate Judge for the Southern District of New York, criminal number 19 Mag. 4784:

iCloud Account	*Owner*	*Referred To As*
[redacted]	Lev Parnas	Subject Account-1
	Lev Parnas	Subject Account-2
	Igor Fruman	Subject Account-3
	[redacted]	Subject Account-4 (collectively, the "Subject Accounts")

II. Review of ESI on the Subject Device

Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, interpreters, and outside vendors or technical experts under government control) are authorized to review the ESI contained on the Subject Accounts for evidence, fruits, and instrumentalities of one or more violations of 18 U.S.C. § 1519 (fabrication of documents); 22 U.S.C. §§ 612 and 618 (failure to register as a foreign agent); 18 U.S.C. § 951 (acting as an agent of a foreign government); and 18 U.S.C. § 1343 (wire fraud) (together, the "Subject Offenses"), as listed below:

a. Evidence related to any false statements or documents made or caused to be made to the Federal Election Commission.

b. Evidence relating to the May 9, 2018 letter from Congressman [redacted] to Secretary of State [redacted] regarding U.S. Ambassador [redacted], including correspondence attaching or concerning the letter.

c. Communications with individuals associated with the government or a political party in the Ukraine, including [redacted].

d. Communications regarding [redacted] specifically or the position of U.S. Ambassador to Ukraine generally.

e. Evidence, including travel records, related to meetings with Ukrainian government officials involving Rudolph Giuliani, [redacted], Parnas, or Fruman.

f. Evidence of knowledge of the foreign agent registration laws and requirements, or lobbying laws, including but not limited to knowledge of the requirement to register as an agent of a foreign principal, or of the prohibition of acting on behalf of, lobbying for, or making contributions on behalf of a foreign principal.

g. Evidence of the intent of Parnas, Igor Fruman, [redacted], David Correia, Andrey Kukushkin, Andrey Muraviev, Giuliani, [redacted] as it relates to the Subject Offenses under investigation.

AO 106 (SDNY Rev. 01/17) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

the Contents of Four iCloud Accounts Currently Located on a Hard Drive

Case No. 19 MAG 9832

APPLICATION FOR A SEARCH AND SEIZURE WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Southern District of New York, there is now concealed *(identify the person or describe the property to be seized)*:

See Attached Affidavit and its Attachment A

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section(s)	*Offense Description(s)*
See Attachment A	

The application is based on these facts:

See Attached Affidavit and its Attachment A

- ☑ Continued on the attached sheet.
- ☑ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

[redacted]
Applicant's signature

Sworn to before me and signed in my presence.

Date: 10/21/2019

Judge's signature

City and state: New York, New York

J. Paul Oetken, United States District Judge
Printed name and title

19 MAG 9832

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of the Application of the United States Of America for a Search Warrant for the Contents of Four iCloud Accounts Currently Located on a Hard Drive Containing the Results of A Prior iCloud Search Warrant, USAO Reference No [redacted]

TO BE FILED UNDER SEAL

Agent Affidavit in Support of Application for a Search Warrant

SOUTHERN DISTRICT OF NEW YORK) ss.:

[redacted], being duly sworn, deposes and says:

I. Introduction

A. Affiant

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). In the course of my experience and training in this position, I have participated in criminal investigations into federal offenses involving public corruption and violations of the federal campaign finance laws. I also have training and experience executing search warrants, including those involving electronic evidence, including emails.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search four iCloud accounts on the electronic device specified below (the "Subject Device") for the items and information described in Attachment A. This affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information ("ESI"). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and